

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-111649

(P2002-111649A)

(43) 公開日 平成14年4月12日 (2002. 4. 12)

(51) Int.Cl.<sup>7</sup>

H 0 4 L 9/08

12/56

識別記号

F I

H 0 4 L 9/00

11/20

テームコード\* (参考)

6 0 1 B 5 J 1 0 4

6 0 1 E 5 K 0 3 0

1 0 2 A

審査請求 有 請求項の数 9 O L (全 7 頁)

(21) 出願番号 特願2000-297847 (P2000-297847)

(22) 出願日 平成12年9月29日 (2000. 9. 29)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 安藤 大介

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 青柳 慎一

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100059258

弁理士 杉村 暁秀 (外1名)

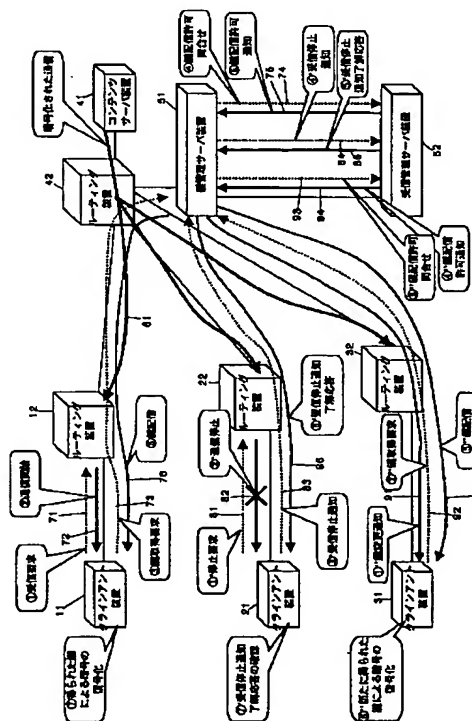
最終頁に続く

(54) 【発明の名称】 マルチキャスト通信方法、サーバ装置及びクライアント装置

(57) 【要約】

【課題】 I G M P を使用するマルチキャスト通信において、マルチキャスト通信データの受信者の管理及び制御を容易に行うことができる方法及び装置を提供する。

【解決手段】 マルチキャストデータを配信するコンテンツサーバ装置、I P レイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含み、コンテンツサーバ装置がマルチキャストデータを暗号化してI P ネットワーク上に配信し、クライアント装置が鍵管理サーバ装置に対して復号化鍵の取得を要求し、鍵管理サーバ装置が受信管理サーバ装置に対して復号化鍵の配信可否を問合わせ、受信管理サーバ装置が復号化鍵の配信を許可し、鍵管理サーバ装置がクライアント装置に対して復号化鍵を配信し、クライアント装置がマルチキャストデータの暗号を復号化する。



## 【特許請求の範囲】

【請求項 1】 マルチキャストデータを配信するコンテンツサーバ装置、IPレイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含むマルチキャスト通信システムにおけるマルチキャスト通信方法であって、

コンテンツサーバ装置がマルチキャストデータを暗号化して IP ネットワーク上に配信し、

クライアント装置が、マルチキャストプロトコルの終端点になっているルーティング装置に対して受信要求を行い、

ルーティング装置は、受信要求を受けると、クライアント装置に対してマルチキャストデータを配信し、

クライアント装置は、鍵管理サーバ装置に対して復号化鍵の取得要求を行い、鍵管理サーバ装置は、復号化鍵の取得要求を受けると、受信管理サーバ装置に対して復号化鍵の配信可否の問い合わせを行い、

受信管理サーバ装置は、復号化鍵の配信可否の問い合わせを受けると、記録されているクライアント装置の受信状況に応じて復号化鍵の配信許可通知を行うと共に受信情報を保持し、

鍵管理サーバ装置は、復号化鍵の配信許可通知を受けると、クライアント装置に対して復号化鍵の配信を行い、クライアント装置は、復号化鍵の配信を受けると、この復号化鍵を利用して、配信されているマルチキャストデータの暗号の復号化を行うことを特徴とするマルチキャスト通信方法。

【請求項 2】 マルチキャストデータを配信するコンテンツサーバ装置、IPレイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含むマルチキャスト通信システムにおけるマルチキャスト通信方法であって、

マルチキャスト通信を停止する場合、

クライアント装置が、マルチキャストプロトコルの終端点になっているルーティング装置に対して受信停止要求を行い、

ルーティング装置は、受信停止要求を受けると、クライアント装置に対してマルチキャストデータの配信の停止を行い、

クライアント装置は、鍵管理サーバ装置に対して受信停止通知を行い、

鍵管理サーバ装置は、クライアント装置から受信停止通知を受けると、受信管理サーバ装置に対して受信停止通知を行い、

受信管理サーバ装置は、受信停止通知を受けると、保持されているクライアント装置の受信情報を削除し、受信

状態の記録を行い、鍵管理サーバ装置に対して受信停止通知了解応答を行い、

鍵管理サーバ装置は、受信停止通知了解応答を受けると、クライアント装置に対して受信停止通知了解応答を行い、

クライアント装置は、受信停止通知了解応答を受けて受信停止の確認を行うことを特徴とするマルチキャスト通信方法。

10 【請求項 3】 マルチキャストデータを配信するコンテンツサーバ装置、IPレイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含むマルチキャスト通信システムにおけるマルチキャスト通信方法であって、

復号化鍵を変更する場合、

コンテンツサーバ装置が暗号化鍵の変更を行い、その変更内容を鍵管理サーバ装置に通知し、

20 鍵管理サーバ装置がその内容を保持し、クライアント装置に対して復号化鍵の変更通知を行い、

クライアント装置は、復号化鍵の変更通知を受けると、鍵管理サーバ装置に対して復号化鍵の取得要求を行い、変更後の復号化鍵を取得することを特徴とするマルチキャスト通信方法。

【請求項 4】 IP を利用するマルチキャスト通信システムにおける暗号化及び復号化鍵を管理するための鍵管理サーバ装置であって、

クライアント装置の復号化鍵の取得要求に応じるための手段、

30 受信管理サーバ装置に対してクライアント装置への復号化鍵の配信の可否を問い合わせるための手段、

受信管理サーバ装置の応答に応じて復号化鍵を配信するための手段、

クライアント装置からマルチキャストデータの受信停止通知を受信するための手段、

受信管理サーバ装置に対してクライアント装置の受信停止通知を行うための手段、

受信管理サーバ装置から受信停止通知了解応答を受信するための手段、及び、クライアント装置に対して受信停止通知了解応答を行うための手段を具えることを特徴とするサーバ装置。

40 【請求項 5】 IP を利用するマルチキャスト通信システムにおけるクライアント装置の受信を管理するための受信管理サーバ装置であって、

鍵管理サーバ装置のクライアント装置への鍵の配信可否の問い合わせに応じるための手段、

問い合わせ内容に応じてクライアント装置の情報を保持するための手段、

鍵管理サーバ装置からクライアント装置の受信停止通知を受信するための手段、

50 受信管理サーバ装置からクライアント装置の受信停止通知を受信するための手段、

鍵管理サーバ装置へ受信停止通知了解応答を行うための手段、

受信停止通知に応じてクライアント装置の保持情報を削除するための手段、及び、

受信停止通知に応じて受信状況を記録するための手段を具えることを特徴とするサーバ装置。

【請求項 6】 IP を利用するマルチキャスト通信システムにおける暗号化及び復号化鍵を管理し、且つ、IP を利用するマルチキャスト通信システムにおけるクライアント装置の受信を管理するためのサーバ装置であって、請求項 4 及び 5 に記載の各手段を具えることを特徴とするサーバ装置。

【請求項 7】 請求項 4 又は 6 に記載のサーバ装置において、更に、

暗号化鍵を一定時間毎に更新するための手段、

更新された暗号化鍵を保持するための手段、及び、

更新内容に応じてマルチキャストデータを受信しているクライアント装置に復号化鍵の変更の通知を行うための手段を具えることを特徴とするサーバ装置。

【請求項 8】 IP を利用するマルチキャスト通信システムにおけるクライアント装置であって、

受信要求を送出するための手段、

鍵管理サーバ装置に対して復号化鍵の取得要求を行うための手段、

得られた復号化鍵を利用してマルチキャストデータの復号化を行うための手段、

受信停止要求を送出するための手段、

鍵管理サーバ装置に対して受信停止通知を行うための手段、及び、

鍵管理サーバ装置から受信停止通知了解応答を受信するための手段を具えることを特徴とするクライアント装置。

【請求項 9】 請求項 8 に記載のクライアント装置において、更に、

鍵管理サーバ装置から復号化鍵の変更通知を受信するための手段、及び、該変更通知に応じて、鍵管理サーバ装置に対して復号化鍵の取得要求を行うための手段を具えることを特徴とするクライアント装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ルーティング装置、スイッチ等を利用する IP ネットワークにおけるデータ通信に関するものであり、特に、ポイント対マルチポイント通信であるマルチキャスト通信の通信方法及び装置に関するものである。

【0002】

【従来の技術】IP ネットワークにおいてポイント対マルチポイント通信を行う場合、ブロードキャスト、マルチキャスト等の技術を使用することができる。特にマルチキャストを使用する場合、受信希望者のみにデータを

送信することができ、帯域の有効利用を図ることができる。このマルチキャストを実現するプロトコルとしては、送信側ベースのプロトコル及び受信側ベースのプロトコルがある。しかしながら、送信側ベースのプロトコルは殆どのルーティング装置及びレイヤ 3 のスイッチに実装されていないため、マルチキャスト通信を行う場合、受信側ベースマルチキャストプロトコル IGMP を使用する場合が多い。

【0003】図 1 は IGMP を使用するマルチキャスト通信方法を説明するための図である。データを受信する場合は、例えば受信を希望するクライアント装置 111 が IGMP の終端点となっているルーティング装置 112 に対して受信要求 142 を行い、ルーティング装置 112 がデータの送信 143 を開始する。また、データの受信を停止する場合は、例えば受信の停止を希望するクライアント装置 121 が IGMP の終端点となっているルーティング装置 122 に対して停止要求 144 を行い、ルーティング装置 122 がデータの送信を停止 145 する。

【0004】このように、IGMP を使用方法においては、クライアントの受信要求及び停止要求は共に IGMP の終端ルーティング装置に対して行うため、送信側のサーバでは通信の管理を行う必要がない。このような方法は、スケーラビリティを考慮の上では有効な方法といえる。

【0005】しかしながら、サーバ側では管理を行わないのでデータ受信を行っているクライアントを把握できない。また、IGMP 自体が受信管理を行う機能を持っておらず、一方、IGMP ルーティング装置は受信クライアントを管理しているが、実際にはクライアントを特定して管理するのではなく、クライアントが所属するサブネットを管理しているため、クライアントの特定は不可能である。このように、IGMP を使用するマルチキャスト通信では、データ受信者の管理及び制御が難しいため、例えば、課金処理を行うことが困難であるという問題があった。

【0006】

【発明が解決しようとする課題】本発明の目的は、上述の問題点に鑑み、IGMP を使用するマルチキャスト通信において、マルチキャスト通信データの受信者の管理及び制御を容易に行うことができる方法及び装置を提供することにある。

【0007】

【課題を解決するための手段】本発明のマルチキャスト通信方法は、マルチキャストデータを配信するコンテンツサーバ装置、IP レイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含むマルチキャスト通信システムにおけるマルチキャスト通信方法であって、コンテンツサーバ装置がマルチキャストデー

タを暗号化してIPネットワーク上に配信し、クライアント装置が、マルチキャストプロトコルの終端点になっているルーティング装置に対して受信要求を行い、ルーティング装置は、受信要求を受けると、クライアント装置に対してマルチキャストデータを配信し、クライアント装置は、鍵管理サーバ装置に対して復号化鍵の取得要求を行い、鍵管理サーバ装置は、復号化鍵の取得要求を受けると、受信管理サーバ装置に対して復号化鍵の配信可否の問い合わせを行い、受信管理サーバ装置は、復号化鍵の配信可否の問い合わせを受けると、記録されているクライアント装置の受信状況に応じて復号化鍵の配信許可通知を行うと共に受信情報を保持し、鍵管理サーバ装置は、復号化鍵の配信許可通知を受けると、クライアント装置に対して復号化鍵の配信を行い、クライアント装置は、復号化鍵の配信を受けると、この復号化鍵を利用して、配信されているマルチキャストデータの暗号の復号化を行うことを特徴とする。

【0008】また、本発明のマルチキャスト通信方法は、マルチキャスト通信を停止する場合、クライアント装置が、マルチキャストプロトコルの終端点になっているルーティング装置に対して受信停止要求を行い、ルーティング装置は、受信停止要求を受けると、クライアント装置に対してマルチキャストデータの配信の停止を行い、クライアント装置は、鍵管理サーバ装置に対して受信停止通知を行い、鍵管理サーバ装置は、クライアント装置から受信停止通知を受けると、受信管理サーバ装置に対して受信停止通知を行い、受信管理サーバ装置は、受信停止通知を受けると、保持されているクライアント装置の受信情報を削除し、受信状態の記録を行い、鍵管理サーバ装置に対して受信停止通知了解応答を行い、鍵管理サーバ装置は、受信停止通知了解応答を受けると、クライアント装置に対して受信停止通知了解応答を行い、クライアント装置は、受信停止通知了解応答を受けて受信停止の確認を行うことを特徴とする。

【0009】また、本発明のマルチキャスト通信方法は、復号化鍵を変更する場合、コンテンツサーバ装置が暗号化鍵の変更を行い、その変更内容を鍵管理サーバ装置に通知し、鍵管理サーバ装置がその内容を保持し、クライアント装置に対して復号化鍵の変更通知を行い、クライアント装置は、復号化鍵の変更通知を受けると、鍵管理サーバ装置に対して復号化鍵の取得要求を行い、変更後の復号化鍵を取得することを特徴とする。

【0010】更に、本発明のIPを利用するマルチキャスト通信システムにおける暗号化及び復号化鍵を管理するための鍵管理サーバ装置は、クライアント装置の復号化鍵の取得要求に応じるための手段、受信管理サーバ装置に対してクライアント装置への復号化鍵の配信の可否を問い合わせるための手段、受信管理サーバ装置の応答に応じて復号化鍵を配信するための手段、クライアント装置からマルチキャストデータの受信停止通知を受信する

ための手段、受信管理サーバ装置に対してクライアント装置の受信停止通知を行うための手段、受信管理サーバ装置から受信停止通知了解応答を受信するための手段、及び、クライアント装置に対して受信停止通知了解応答を行うための手段を具えることを特徴とする。

【0011】また、本発明の鍵管理サーバ装置は、更に、暗号化鍵を一定時間毎に更新するための手段、更新された暗号化鍵を保持するための手段、及び、更新内容に応じてマルチキャストデータを受信しているクライアント装置に復号化鍵の変更の通知を行うための手段を具えることができる。

【0012】更に、本発明のIPを利用するマルチキャスト通信システムにおけるクライアント装置の受信を管理するための受信管理サーバ装置は、鍵管理サーバ装置のクライアント装置への鍵の配信可否の問い合わせに応じるための手段、問い合わせ内容に応じてクライアント装置の情報を保持するための手段、鍵管理サーバ装置からクライアント装置の受信停止通知を受信するための手段、鍵管理サーバ装置へ受信停止通知了解応答を行うための手段、受信停止通知に応じてクライアント装置の保持情報を削除するための手段、及び、受信停止通知に応じて受信状況を記録するための手段を具えることを特徴とする。

【0013】更に、本発明のIPを利用するマルチキャスト通信システムにおけるクライアント装置は、受信要求を送出するための手段、鍵管理サーバ装置に対して復号化鍵の取得要求を行うための手段、得られた復号化鍵を利用してマルチキャストデータの復号化を行うための手段、受信停止要求を送出するための手段、鍵管理サーバ装置に対して受信停止通知を行うための手段、及び、鍵管理サーバ装置から受信停止通知了解応答を受信するための手段を具えることを特徴とする。

【0014】また、本発明のクライアント装置は、更に、鍵管理サーバ装置から復号化鍵の変更通知を受信するための手段、及び、変更通知に応じて、鍵管理サーバ装置に対して復号化鍵の取得要求を行うための手段を具えることができる。

#### 【0015】

【発明の実施の形態】次に、本発明の実施例を説明する。図2は本発明の実施例を説明するための図であり、受信側ベースマルチキャストプロトコルIGMPを使用するコンテンツ配信IPネットワークの構成を示す図である。図に示されたIPネットワークには、マルチキャストデータを配信するコンテンツサーバ装置41、IPレイヤのルーティング装置12、22、32、42、暗号化及び復号化鍵を管理する鍵管理サーバ装置51、クライアント装置を管理する受信管理サーバ装置52、マルチキャストデータを受信するクライアント装置11、21、31が含まれている。マルチキャストデータは、暗号化されて、コンテンツサーバ装置41からIPネットワーク内に配信61され

る。

【0016】次に、例えばクライアント装置11が、マルチキャストデータを受信する場合の動作を説明する。クライアント装置11が、マルチキャストプロトコルの終端点になっているルーティング装置12に対して受信要求71を行う。ルーティング装置12は、受信要求を受けると、クライアント装置11に対してマルチキャストデータの配信72を開始する。その後、クライアント装置11は、鍵管理サーバ装置51に対して復号化鍵の取得要求73を行う。鍵管理サーバ装置51は、復号化鍵の取得要求を受けると、受信管理サーバ装置52に対して復号化鍵の配信可否の問い合わせ74を行う。受信管理サーバ装置52は、復号化鍵の配信可否の問い合わせを受けると、記録されているクライアント装置11の受信状況に応じて復号化鍵の配信許可通知75を行うと共に受信情報を保持する。受信管理サーバ装置52は、復号化鍵の配信許可通知を受けると、クライアント装置11に対して復号化鍵の配信76を行う。クライアント装置11は、復号化鍵の配信を受けると、この復号化鍵を利用して、配信されているマルチキャストデータの暗号の復号化を行う。

【0017】次に、例えばクライアント装置21が、受信しているマルチキャストデータの受信停止を行う場合の動作を説明する。クライアント装置21が、マルチキャストプロトコルの終端点になっているルーティング装置22に対して受信停止要求81を行う。ルーティング装置22は、受信停止要求を受けると、クライアント装置21に対してマルチキャストデータの配信の停止82を行う。その後、クライアント装置21は、鍵管理サーバ装置51に対して受信停止通知83を行う。鍵管理サーバ装置51は、クライアント装置21から受信停止通知を受けると、受信管理サーバ装置52に対して受信停止通知84を行う。受信管理サーバ装置52は、受信停止通知を受けると、保持されているクライアント装置21の受信情報を削除し、受信状態の記録を行い、鍵管理サーバ装置51に対して受信停止通知了解応答85を行う。鍵管理サーバ装置51は、受信停止通知了解応答を受けると、クライアント装置21に対して受信停止通知了解応答86を行う。クライアント装置21は、受信停止通知了解応答を受けて受信停止の確認を行う。

【0018】次に、マルチキャストデータを暗号化及び復号化鍵を変更する場合の動作を説明する。暗号化及び復号化鍵の変更は、例えば一定時間毎に、コンテンツサーバ装置が行い、その変更内容を鍵管理サーバ装置に通知し、鍵管理サーバ装置がその内容を保持する。例えばクライアント装置31が、復号化鍵の変更が行われるマルチキャストデータを受信しているとする。鍵管理サーバ装置51が、クライアント装置31に対して復号化鍵の変更通知91を行う。クライアント装置31は、復号化鍵の変更通知を受けると、鍵管理サーバ装置51に対して復号化鍵の取得要求92を行う。鍵管理サーバ装置51は、復号化鍵

の取得要求を受けると、受信管理サーバ装置52に対して復号化鍵の配信可否の問い合わせ93を行う。受信管理サーバ装置52は、復号化鍵の配信可否の問い合わせを受けると、記録されているクライアント装置31の受信状況に応じて復号化鍵の配信許可通知94を行うと共に受信情報を保持する。受信管理サーバ装置52は、復号化鍵の配信許可通知を受けると、クライアント装置31に対して復号化鍵の配信95を行う。クライアント装置31は、復号化鍵の配信を受けると、新たに得られたこの復号化鍵を利用して、配信されているマルチキャストデータの暗号の復号化を行う。

【0019】以上の例によれば、鍵管理サーバ装置及び受信管理サーバ装置が、マルチキャストデータのマルチキャストプロトコルの受信要求、受信停止要求及び復号化鍵の取得要求を受付けて処理することにより、これらの装置によりクライアント装置の受信状況の管理及び制御を行うことが可能になる。

【0020】上述の例では、IPネットワークが各1台のコンテンツサーバ装置、鍵管理サーバ装置及び受信管理サーバ装置を含む場合を示したが、IPネットワークがこれらの装置を複数含んでもよいことは勿論である。また、3台のクライアント装置及び4台のルーティング装置を示したが、この数は限定されないことも勿論である。また、マルチキャストプロトコルの終端点にあるルーティング装置配下には各1台のクライアント装置が接続されている例を示したが、この数は限定されないことも勿論である。また、上述では鍵管理サーバ装置と受信管理サーバ装置とが別装置である例を説明したが、両者の機能を含むサーバ装置としてもよいことは勿論である。

【0021】更に、本発明は、ルーティング装置相互間、ルーティング装置とクライアント装置との間、ルーティング装置とコンテンツサーバ装置との間、ルーティング装置と鍵管理サーバ装置との間、及び、鍵管理サーバ装置と受信管理サーバ装置との間の通信線、通信方法及び通信装置には依存しない。また、コンテンツサーバ装置から配信されるコンテンツは、ブロックデータ、ストリーム等、どのような種類のデータであってもよい。また、クライアント装置における、マルチキャストプロトコルによる受信要求と復号化鍵の取得要求との順序は、上述の例に限定されるものではなく任意に定めることができる。同様に、クライアント装置における、マルチキャストプロトコルによる受信停止要求と鍵管理サーバ装置への受信停止通知との順序は、上述の例に限定されるものではなく任意に定めることができる。

【0022】

【発明の効果】以上説明したように、本発明によれば、マルチキャスト通信において、受信側ベースのマルチキャストプロトコルを使用し、暗号化及び復号化を管理する鍵管理サーバを組合せることにより、従来不可能であ

ったマルチキャスト通信データの受信者に関する管理及び制御が可能になる。

【図面の簡単な説明】

【図1】 IGMPを使用するマルチキャスト通信方法を説明するための図である。

【図2】 本発明の実施例を説明するための図である。

【符号の説明】

11、21、31 クライアント装置

12、22、32、42 ルーティング装置

41 コンテンツサーバ装置

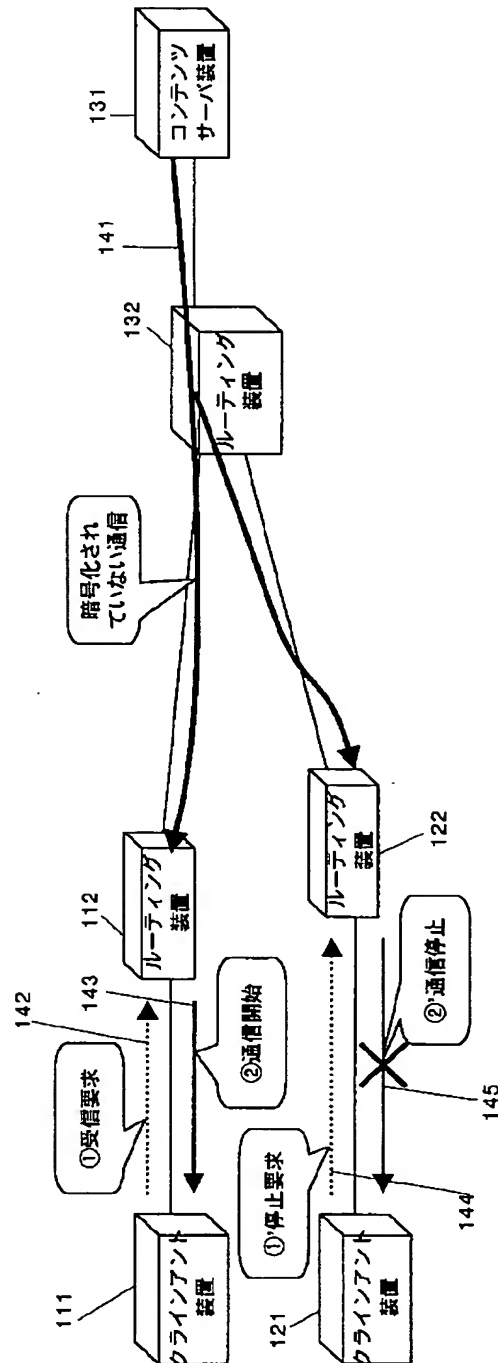
51 鍵管理サーバ装置

52 受信管理サーバ装置

111、121、131 クライアント装置

112、122、132 ルーティング装置

【図1】



【図2】

